UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,904	06/28/2001	Yves Louis Gabriel Audebert	L741.01105	1582

7590 10/14/2004

STEVENS, DAVIS, MILLER & MOSHER, LLP
Suite 850
1615 L Street, N.W.
Washington, DC 20036

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,904	AUDEBERT ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 9/28/2001, 3/28/20.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are presented for examination.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 13, 14, and 15 rejected under 35 U.S.C. 102(e) as being anticipated by Thomlinson et al. (Thomlinson, Patent No.: US 6,389,535 B1).

4.1 As per claim 13, Thomlinson teaches a data processing system for validating a key protection certificate (Thomlinson Col. 4 lines 8-25) comprising;

data processing means (Thomlinson Fig. 2), data storage means (Thomlinson Fig. 1 No. 22), communications means (Thomlinson Fig. 1 No. 46), cryptography means (Thomlinson Fig. 1 No. 37, col. 2 lines 8-16), a first securely shared secret symmetric key, a second securely shared secret symmetric key and a public key (Thomlinson Col. 3 lines 40-45), wherein the cryptography means includes a message authentication code algorithm (Thomlinson Fig. 3 No. 133), cross referencing means and a comparator algorithm (Thomlinson Col. 4 lines 1-12).

4.2 As per claim 14, Thomlinson teaches the system, wherein said first symmetric key, said second symmetric key and said public key have a direct generation relationship with said key protection certificate (Thomlinson Col. 4 lines 27-33, Col. 3 lines 41-44).

4.3 As per claim 15, Thomlinson teaches the system, wherein said communications means includes means for transmitting requests for said key protection certificate and said public key and means for receiving said key protection certificate and said public key (Thomlinson Col. 4 lines 27-34).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-12, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chasko et al. (Chasko Patent No.: US 6,715,078 B1) in view of Schneck et al. (Schneck Pub. No.: US 2001/0021926 A1)

6.1 As per claim 1, Chasko teaches a data processing system for generating a key protection certificate comprising:

a PSD further comprising a unique device name (Chasko fig. 2 No. 202; smart card serial number), cryptography means (Chasko Fig. 2 No. 205; encryption algorithms and keys for cryptography), data processing means (Chasko Fig. 2 No. 204), data storage means and communications means (Chasko Col. 5 lines 25-45);

wherein said cryptography means includes an asymmetric key pair generating algorithm, a first securely shared secret key, a second securely shared secret key, symmetric cryptography means (Chasko Col. 5 lines 44-56; DES key sharing), a concatenation algorithm (Chasko Fig. 4 No. 408; Smart card combines the cryptographic serial number with random seed), a message authentication code algorithm (Chasko Col. 1 lines 58-col. 2 lines 5), cryptographic seed information (Chasko Col. 6 lines 43-64),

Chasko does not explicitly teach a key protection certificate algorithm and a signing algorithm.

However Schneck teaches a key protection certificate algorithm (Schneck Page 12 par. 0188) and a signing algorithm (Schneck Page 16 par. 0281, page 13 par. 0224).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneck with in the system of Chasko because it would allow to issue a certificate by a trusted party and include a decryption key therein (Schneck Page 12 par. 0187). A trusted authority issues a certificate to insure the third party by saying the key is protected or not tampered by unauthorized party. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to ensure the third parties by issuing a certificate, and certify the installed cryptography keys are securely stored and have not been replaced or duplicated by another unauthorized device because Schneck teaches issuing a certificate to ensure the third party that the keys are secured and not changed by unauthorized user.

6.2 As per claim 26, Chasko teaches a method for generating a key protection certificate comprising:

injecting a first securely shared secret symmetric key, a second securely shared secret symmetric key (Chasko Col. 5 lines 44-56), a key protection algorithm and cryptographic seed information into a PSD (Chasko Col. 4 lines 33-58), wherein at least a portion of said seed

information is used in generating at least one public key and one private key (Chasko Col. 6 lines 43-64),

storing said injected symmetric keys and said seed information in a secure domain within said PSD (Chasko Col. 4 lines 59-67),

generating said at least one public key and said one private key using at least a portion of said seed information (Chasko Col. 4 lines 33-58, Col. 5 lines 44-56),

storing said public key and said private key in said secure domain (Chasko Col. 4 lines 59-67),

Chasko does not explicitly teach sending a command to said PSD for generating said at least one public key and one private key, wherein said command initiates generation of said keys and of said key protection certificate,

generating contextual attributes specific to at least the generation of said private key,

encrypting at least a portion of said contextual attributes using said first shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in said private contextual attributes,

generating a digital signature of a unique device name using said private key, concatenating said device name, private contextual attributes, public contextual attributes with said digital signature and generating a first intermediate result,

generating a message authentication code of said first intermediate result using said second shared secret key producing a second intermediate result,

concatenating said first intermediate result with said second intermediate result producing said key protection certificate; and

storing said key protection certificate in said secure domain.

However Schneck teaches sending a command to said PSD for generating said at least one public key and one private key, wherein said command initiates generation of said keys and of said key protection certificate (Schneck Page 12 par. 0188),

generating contextual attributes specific to at least the generation of said private key (Schneck page 6 par. 0094 Fig. 2, & 3),

encrypting at least a portion of said contextual attributes using said first shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in said private contextual attributes (Schneck page 6 par. 0094 Fig. 2, & 3, and page 7 par. 0106),

generating a digital signature of a unique device name using said private key (Schneck Page 6 par. [0279-0281],

concatenating said device name, private contextual attributes, public contextual attributes with said digital signature and generating a first intermediate result (Schneck Page 16 par. [0279-0281],

generating a message authentication code of said first intermediate result using said second shared secret key producing a second intermediate result (Schneck Page 16 par. 0279),

concatenating said first intermediate result with said second intermediate result producing said key protection certificate (Schneck Page 12 par. 0188); and

storing said key protection certificate in said secure domain (Schneck Page 12 par. 0187).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneck with in the system of Chasko because it would allow to issue a certificate by a trusted party and include a decryption key therein (Schneck Page 12 par. 0187). A trusted authority issues a certificate to insure the third party by saying the key is protected or not tampered by unauthorized party. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to ensure the third parties by issuing a certificate, and certify the installed cryptography keys are securely stored and have not been replaced or duplicated by another unauthorized device because Schneck teaches issuing a certificate to ensure the third party that the keys are secured and not changed by unauthorized user.

6.3 As per claim 2, Chasko and Schneck teach all the subject matter as described above. In addition Chasko teaches the system, wherein at least a portion of said cryptographic seed information is used by said asymmetric key pair generating algorithm to generate at least one asymmetric private key and one asymmetric public key upon receipt of at least one key generation command, said keys being stored in a secure domain (Chasko Col. 5 lines 44-56).

6.4 As per claim 3, Chasko and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said key protection certificate algorithm, upon

receipt of said key generation command, generates a plurality of contextual attributes (Schneck Fig. 2, & 3, and Page 6 par. 0094). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneck with in the system of Chasko because contextual attributes would allow to validate the integrity of the data file.

6.5 As per claim 4, Chasko and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein at least a portion of said contextual attributes are encrypted using said first shared secret key and said symmetric cryptography means to generate private contextual attributes (Schneck Fig. 2, Page 7 par. 0106) Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneck with in the system of Chasko because it would allow to protect private data from unauthorized users tampering the data.

6.6 As per claim 5, Chasko and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein the remaining unencrypted of said plurality of said contextual attributes forms public contextual attributes (Schneck Fig. 2 No. 122) The rational for combining are the same as claim 1 above.

6.7 As per claim 6, Chasko and Schneck teach all the subject matter as described above. In addition Chasko teaches the system, wherein a signed device name is generated using said unique device name (Chasko Fig. 2 No. 202, 203) and said asymmetric private key as inputs into

said signing algorithm (Chasko Col. 5 lines 44-56).

6.8 As per claim 7, Chasko and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said private contextual attributes, public contextual attributes, signed device name and unique device name are concatenated by said concatenation algorithm, generating a first intermediate result (Schneck Page 16 par. 0281, Page 6 par. 0094) The rational for combining are the same as claim 1 above.

6.9 As per claim 8, Chasko and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein a message authentication code is generated using said second shared secret key and said first intermediate result as inputs into said message authentication code algorithm, forming a second intermediate result (Schneck Page 12 par. 0188) The rational for combining are the same as claim 1 above.

6.10 As per claim 9, Chasko and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said first intermediate result and said second intermediate result are concatenated by said concatenation algorithm forming said key protection certificate then stored in said secure domain (Schneck Par. 12 [0187-0188]) The rational for combining are the same as claim 1 above.

6.11 As per claim 10, Chasko and Schneck teach all the subject matter as described above. In addition Chasko teaches the system, wherein said unique device name is an embedded serial

number (Chasko fig. 2 No. 202).

6.12 As per claim 11, Chasko and Schneck teach all the subject matter as described above. In addition Chasko teaches the system, wherein said unique device name is the result of a cryptographic process using said embedded serial number as a cryptographic seed (Chasko Col. 4 lines 32-58).

6.13 As per claim 12, Chasko and Schneck teach all the subject matter as described above. In addition Chasko teaches the system, wherein said communications means includes means for receiving commands to generate asymmetric and symmetric keys and means for sending said public key and said key protection certificate (Chasko Col. 5 lines 24-44).

7. Claims 16-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al. (Thomlinson, Patent No.: US 6,389,535 B1) in view of Schneck et al. (Schneck Pub. No.: US 2001/0021926 A1).

7.1 As per claim 16, Thomlinson teaches all the subject matter as described above.

Thomlinson does not explicitly disclose the system, wherein said received key protection certificate includes private contextual attributes, public contextual attributes, a device name, a signed device name and a message authentication code.

However Schneck teaches the system, wherein said received key protection certificate includes private contextual attributes, public contextual attributes, a device name, a signed device name and a message authentication code (Schneck Fig. 2 & 3, and Page 12 par. 0188).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneck with in the system of Thomlinson because it would allow to authenticate digital information by providing proof that information received is precisely that which was sent, with no changes (Schneck Page 16 par. 0279).

7.2 As per claim 17, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said device name is used by said cross referencing means for selecting the proper shared secret keys, public key, cryptographic algorithms and reference parameters associated with said key protection certificate (Schneck Page 8 par. 0122) The rational for combining are the same as claim 16 above.

7.3 As per claim 18, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said signed device name is decrypted using said public key, generating a second device name (Schneck Page 11 par. 0168) The rational for combining are the same as claim 16 above.

7.4 As per claim 19, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said second device name and said device name contained in said certificate are compared by the comparator algorithm to

determine if said second device name and said device name contained in said certificate match (Schneck Page 11 par. 0168, page 18 par. 0318) The rational for combining are the same as claim 16 above.

7.5 As per claim 20, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein a second message authentication code is generated using said private contextual attributes, public contextual attributes, device name, said signed device name included in said certificate and said second shared secret key as inputs into said message authentication code algorithm (Schneck Fig. 2, &3 par. 0094, page 7 par. 0106) The rational for combining are the same as claim 16 above.

7.6 As per claim 21, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said second message authentication code and said message authentication code contained in said certificate are compared using said comparator algorithm to determine if said second message authentication code and said message authentication code contained in said certificate match (Schneck Page 11 par. 0168, page 16 par. 0281) The rational for combining are the same as claim 16 above.

7.7 As per claim 22, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein said private contextual attributes are decrypted using said first shared secret key (Schneck Page 10 par. 0143, page 12 par. 0188).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneck with in the system of Thomlinson because it would allow to protect digital data by encrypting the portion of the data, (Schneck Page 4 par. 0053) and generates digital signature to ensure the third person that the data is not accessed by unauthorized person.

7.8 As per claim 23, Thomlinson and Schneck teach all the subject matter as described above. In addition Schneck teaches the system, wherein at least one predetermined parameter is contained in at least a portion of said decrypted private contextual attributes (Schneck Page 5 par. 0087, Fig. 2 & 3) The rational for combining are the same as claim 22 above.

7.9 As per claim 24, Thomlinson and Schneck teach all the subject matter as described above. In addition, Thomlinson teaches the system, wherein at least one predetermined parameter and said reference parameters are compared using said comparator algorithm to determine if said at least one predetermined parameter and said reference parameters match (Thomlinson Col. 4 lines 13-26, col. 11 lines 6-18, col. 13 lines 21-47).

7.10 As per claim 25, Thomlinson and Schneck teach all the subject matter as described above. In addition, Thomlinson teaches the system according to claim 19, 21 or 24, wherein a failure to achieve a match invalidates said key protection certificate (Thomlinson Col. 13 lines 34-47, col. 12 lines 43-67).

8. Claims 27, 28, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneck et al. (Schneck Pub. No.: US 2001/0021926 A1) in view of Nakamura et al. (Nakamura, Patent No.: US 6,415,371 B1)

8.1 As per claim 27, Schneck teaches method for validating a key protection certificate comprising:

receiving said key protection certificate and a public key (Schneck Page 12 par. 0188), wherein said certificate contains at least a plain text device name portion, a signed device name portion and cryptogram portion (Schneck Page 16 par. 0281),

cross-referencing said device name with proper shared secret keys, public key, cryptographic algorithms and reference parameters associated with said key protection certificate (Schneck Page 16 par. 0281),

verifying said signed device name portion of said certificate using said public key (Schneck Page 16 par. 0281, page 8 par. 0122),

comparing the resulting device name with said device name portion included in said certificate (Schneck Page 16 par. 0279),

independently performing a message authentication code function on said concatenated private contextual attributes, public contextual attributes, device name, and signed device name portions of said certificate using a first of said shared secret keys (Schneck Page 16 par. 0281, page 17 par. 0283, page 7 par. 0106),

comparing the resulting message authentication code with a method authentication code included in said certificate (Schneck Page 16 par. 0271, par. 0281),

decrypting said private contextual attributes using a second of said shared secret keys (Schneck Page 10 par. 0143, page 12 par. 0188),

comparing at least a portion of the private contextual attributes to the reference parameters (Schneck Page 16 par. 0279),

validating said certificate if said resulting device name matches said device name contained in said certificate (Schneck Page 12 par. 0187), said independently generated message authentication code matches said message authentication code contained in said certificate and at least a portion of said private contextual attributes matches said reference parameter (Schneck Page 16 par. [0279-0281],

Schneck does not explicitly teach rejecting said certificate if any of said matches is not achieved.

However Nakamura teaches rejecting certificates when certification data does not coincide with the data stored on the storage medium (Nakamura Col. 6 lines 27-33)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Nakamura with in the system of Schneck because it would provide a method for protecting data, so that stored data is so encoded as to be accordance with an easy process (Nakamura Page 1 lines 48-54)

8.2 As per claim 28, Schneck teaches the method, wherein said receiving party possesses said

securely shared secret keys and said public key (Schneck Page 5 par. 0070).

8.3 As per claim 29, Schneck teaches the method, wherein said receiving party is a trusted third party certificate authority (Schneck Page 12 par. 0187).

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100